In the Claims

The status of claims in the case is as follows:

1. [Currently amended] A method for providing local gateway support for multiple overlapping remote networks using source-in VPN NAT, comprising the steps of:

loading a plurality of overlapping connections, each including an inbound packet having a conflicting source IP address;

for each said connection, binding said source IP address or VPN connection name in a bind table with an internally routable and system-wide unique source IP address from an internal address pool; and

VPN network address translating outbound packets, each said outbound packet having a destination IP address, to determine a virtual private network connection for receiving said outbound packet.

2. [Currently amended] ~~The method of claim 1, further~~

~~comprising the steps of:~~ A method for providing local gateway support for multiple overlapping remote networks, comprising the steps of:

loading a plurality of overlapping connections, each including an inbound packet having a source IP address;

for each said connection, binding said source IP address in a bind table with an internally routable and system-wide unique source IP address from an internal address pool;

network address translating outbound packets, each said outbound packet having a destination IP address, to determine a virtual private network connection for receiving said outbound packet;

filtering said outbound packet to determine a first connection name;

determining from said bind table a second connection name;

responsive to said first and second connection names

comparing equal, processing said outbound packet into a VPN tunnel using a security association database determined by said first connection name; and

responsive to said first and second connection names comparing not equal, processing said outbound packet into a VPN tunnel using a security association database determined by said second connection name.

3. [Original] A local gateway system, comprising:

an address pool for storing a plurality of internally routable and system wide, nonconflicting network addresses;

an address bind table for binding a conflicting source address from an inbound packet from a remote network to a connection name and to a unique network address from said address pool;

a filter rules table responsive to an outbound packet for determining a first connection indicia;

said address bind table further responsive to said

outbound packet for determining a second connection indicia; and

said local gateway system being responsive to said first and second connection indicia comparing equal for processing said outbound packet to a communications tunnel using a first security association determined by said first connection indicia, and responsive to said first and second connection indicia comparing not equal for processing said outbound packet to a communications tunnel using a second security association determined by said second connection indicia.

4. [Currently amended] A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for providing local gateway support for multiple overlapping remote networks using source-in VPN NAT, said method steps comprising:

loading a plurality of overlapping connections, each including an inbound packet having a conflicting source IP address;

for each said connection, binding said source IP address in a bind table with an internally routable and system-wide unique source IP address from an internal address pool; and

VPN network address translating outbound packets, each said outbound packet having a destination IP address, to determine a virtual private network connection for receiving said outbound packet.

5. [Currently amended] ~~The program storage device of claim 4, said method steps further comprising.~~ A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for providing local gateway support for multiple overlapping remote networks, said method steps comprising:

loading a plurality of overlapping connections, each including an inbound packet having a source IP address;

for each said connection, binding said source IP address in a bind table with an internally routable and system-wide unique source IP address from an internal

address pool;

network address translating outbound packets, each said outbound packet having a destination IP address, to determine a virtual private network connection for receiving said outbound packet;

filtering said outbound packet to determine a first connection name;

determining from said bind table a second connection name;

responsive to said first and second connection names comparing equal, processing said outbound packet into a VPN tunnel using a security association database determined by said first connection name; and

responsive to said first and second connection names comparing not equal, processing said outbound packet into a VPN tunnel using a security association database determined by said second connection name.

6. [Currently amended] A computer program product or

computer program element for providing local gateway support for multiple overlapping remote networks using source-in VPN NAT, according to method steps comprising:

loading a plurality of overlapping connections, each including an inbound packet having a conflicting source IP address;

for each said connection, binding said source IP address in a bind table with an internally routable and system-wide unique source IP address from an internal address pool; and

VPN network address translating outbound packets, each said outbound packet having a destination IP address, to determine a virtual private network connection for receiving said outbound packet.

7. [Original] A local gateway system for processing inbound and outbound packets with respect to a local network and a plurality of remote nodes having potentially overlapping addresses, comprising:

an address pool component;

an address bind table component;

a filter rules table component;

a security association component;

an entry in said address bind table component including a left hand side (LHS) address field, a right hand side (RHS) address field, and first connection name field;

an entry in said filter rules table component including source IP address (sip), destination IP address (dip), source port, destination port, second connection name, and action field;

said address pool component including a pool of sip addresses administratively reserved and uniquely routable within said local network;

a security association in said security association component including third connection name and security association data;

first logic responsive to an inbound packet for

dynamically binding in said address bind table component the inbound packet sip with a local sip selected from said address pool component and first connection indicia;

second logic responsive to an outbound packet for accessing said filter rules table component to determine filter derived connection indicia;

third logic responsive to said outbound packet for accessing said address bind table component to determine corresponding bind table derived connection indicia; and

fourth logic responsive to said filter derived connection indicia and said bind table derived connection indicia comparing equal for accessing said security association component to select security association data corresponding to said filter derived connection data for processing said outbound packet, and responsive to said filter derived connection indicia and said bind table derived connection indicia comparing not equal for accessing said security association component to select security association

data corresponding to said bind table derived connection indicia for processing said outbound packet.

8. [Original] The local gateway system of claim 7, further comprising:

said action field selectively containing deny, permit, and IP Sec required indicia; and

said second logic being responsive to said outbound packet corresponding to a filter having an action field containing said IP Sec required indicia for initiating execution of said third logic.

9. [Currently amended] A method for operating a local gateway using source-in VPN NAT, comprising the steps of:

receiving an inbound packet having a conflicting source-in IP address on a network connection from a remote node; and

applying source-in network address translation to establish dynamic binding of the source IP address of said inbound packet with an internally routable and

system wide unique source-in IP address and a connection name.

10. [Currently amended] ~~The method of claim 9, further comprising the steps of:~~ A method for operating a local gateway, comprising the steps of:

receiving an inbound packet on a network connection from a remote node;

applying source-in network address translation to establish dynamic binding of the source IP address of said inbound packet with an internally routable and system wide unique source-in IP address and a connection name;

receiving an outbound packet from an internal node;

filtering said outbound packet to determine a first connection;

selectively determining a second connection from a connection name bound to said unique source-in IP address corresponding to the destination-out IP address

of said outbound packet; and

selectively overriding said first connection by said second connection.

11. [Original] The method of claim 10, further comprising the step of:

tunneling said outbound packet to said remote node responsive to security association data selectively corresponding to said first connection or said second connection.

12. [Original] The method of claim 11, further comprising the step of:

overriding said first connection by said second connection responsive to said first connection and said second connection comparing not equal.

13. [Currently amended] A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for providing local gateway support for multiple overlapping

remote networks using source-in VPN NAT, said method steps comprising:

receiving an inbound packet having a conflicting source-in IP address on a network connection from a remote node; and

applying VPN source-in network address translation to establish dynamic binding of the source IP address of said inbound packet with an internally routable and system wide unique source-in IP address and a connection name.

14. [Currently amended] ~~The program storage device of claim 13, said method steps further comprising:~~ A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for providing local gateway support for multiple overlapping remote networks, said method steps comprising:

receiving an inbound packet on a network connection from a remote node;

applying source-in network address translation to establish dynamic binding of the source IP address of said inbound packet with an internally routable and system wide unique source-in IP address and a connection name;

receiving an outbound packet from an internal node;

filtering said outbound packet to determine a first connection;

selectively determining a second connection from a connection name bound to said unique source-in IP address corresponding to the destination-out IP address of said outbound packet; and

selectively overriding said first connection by said second connection.

15. [Original] The program storage device of claim 14, said method steps further comprising:

tunneling said outbound packet to said remote node responsive to security association data selectively

corresponding to said first connection or said second connection.

16. [Original] The program storage device of claim 15, said method steps further comprising:

overriding said first connection by said second connection responsive to said first connection and said second connection comparing not equal.

17. [Original] A communication method, comprising the steps of:

operating a remote gateway to initiate a connection with a local gateway;

sending from a remote node at said remote gateway an inbound packet addressed by a destination address to a local node at said local gateway and a remote node source address identifying said remote node;

operating said local gateway to decapsulate said inbound packet;

operating said local gateway to determine that said inbound packet requires source-in network address translation and that no existing address bind exists for said inbound packet;

operating said local gateway to choose a pool address and create a binding table entry binding said remote node source address to said pool address and a unique connection name;

replacing said remote node source address with said pool address and forwarding said inbound packet to said local node;

receiving at said local gateway an outbound packet having as its destination address said pool address;

filtering said outbound packet to identify corresponding connection indicia;

finding in said binding table an entry corresponding to said outbound packet, converting said destination address to said remote node source address, and returning said unique connection name;

responsive to said unique connection name, selecting security association data; and

responsive to said security association data, tunneling said outbound packet to said remote node.

18. [Original] The method of claim 17, said remote node being one of a plurality of remote nodes having overlapping addresses.

19. [Original] The method of claim 18, further comprising the steps of:

comparing said corresponding connection indicia and said unique connection name; and

responsive to said corresponding connection indicia and said unique connection name comparing equal, selecting security association data corresponding to said corresponding connection indicia.

20. [Currently amended] A method for operating a local gateway for controlling communication between a local node and a remote node using source-in VPN NAT, comprising the

steps of:

receiving an inbound packet on a network connection from a remote node, said inbound packet characterized by a conflicting first source address identifying said remote node and a first destination address identifying said local node; and

applying VPN source-in network address translation to establish dynamic binding of said first source address with an internally routable and system wide unique second source address and a first connection name.

21. [Currently amended] ~~The method of claim 20, further comprising the steps of:~~ A method for operating a local gateway for controlling communication between a local node and a remote node, comprising the steps of:

receiving an inbound packet on a network connection from a remote node, said inbound packet characterized by a first source address identifying said remote node and a first destination address identifying said local node;

applying source-in network address translation to establish dynamic binding of said first source address with an internally routable and system wide unique second source address and a first connection name; and

establishing said dynamic binding by creating a binding entry in an address bind table with a bind entry left hand side set equal to said second source address selected from a local address pool, a bind entry right hand side set equal to said first source address, and said first connection name.

22. [Original] The method of claim 21, further comprising the steps of:

receiving from said local node an outgoing packet intended for said remote node and having identifying indicia including a second destination address;

filtering said outgoing packet to find a filter rule having a second connection name associated with said identifying indicia;

responsive to said second connection name, identifying

a filter derived security association;

responsive to said filter rule requiring source-in network address translation, searching said address bind table for a matching binding entry having a bind entry left hand side corresponding to said second destination address, and setting said second destination address equal to said bind entry right hand side;

responsive to said first connection name selected from said matching binding entry, identifying a binding table derived security association; and

selectively responsive to said filter derived security association or said binding table derived security association, processing said outbound packet into a tunnel for communication to said remote node.

23. [Original] The method of claim 22, further comprising the steps of:

responsive to said first connection name selected from said matching binding entry and said second connection

name comparing not equal, selecting said binding table derived security association for processing said outbound packet.

24. [Original] A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for providing local gateway support for multiple overlapping remote networks, said method steps comprising:

operating a remote gateway to initiate a connection with a local gateway;

sending from a remote node at said remote gateway an inbound packet addressed by a destination address to said local node at said local gateway and a remote node source address identifying said remote node;

operating said local gateway to decapsulate said inbound packet;

operating said local gateway to determine that said inbound packet requires source-in network address translation and that no existing address bind exists

for said inbound packet;

operating said local gateway to choose a pool address and create a binding table entry binding said remote node source address to said pool address and a unique connection name;

replacing said remote node source address with said pool address and forwarding said inbound packet to said local node;

receiving at said local gateway an outbound packet having as its destination address said pool address;

filtering said outbound packet to identify corresponding connection indicia;

finding in said binding table an entry corresponding to said outbound packet, converting said destination address to said remote node source address, and returning said unique connection name;

responsive to said unique connection name, selecting security association data; and

responsive to said security association data, tunneling said outbound packet to said remote node.

25. [Currently amended] A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for providing local gateway support for multiple overlapping remote networks using source-in VPN NAT, said method steps comprising:

receiving an inbound packet on a network connection from a remote node, said inbound packet characterized by a conflicting first source address identifying said remote node and a first destination address identifying said local node; and

applying VPN source-in network address translation to establish dynamic binding of said first source address with an internally routable and system wide unique second source address and a first connection name.

26. [Currently amended] ~~The program storage device of claim 25, said method steps further comprising:~~ A program storage device readable by a machine, tangibly embodying a

program of instructions executable by a machine to perform method steps for providing local gateway support for multiple overlapping remote networks, said method steps comprising:

receiving an inbound packet on a network connection from a remote node, said inbound packet characterized by a first source address identifying said remote node and a first destination address identifying said local node;

applying source-in network address translation to establish dynamic binding of said first source address with an internally routable and system wide unique second source address and a first connection name; and

establishing said dynamic binding by creating a binding entry in an address bind table with a bind entry left hand side set equal to said second source address selected from a local address pool, a bind entry right hand side set equal to said first source address, and said first connection name.

27. [Original] The program storage device of claim 26,

said method steps further comprising:

receiving from said local node an outgoing packet intended for said remote node and having identifying indicia including a second destination address;

filtering said outgoing packet to find a filter rule having a second connection name associated with said identifying indicia;

responsive to said second connection name, identifying a filter derived security association;

responsive to said filter rule requiring source-in network address translation, searching said address bind table for a matching binding entry having a bind entry left hand side corresponding to said second destination address, and setting said second destination address equal to said bind entry right hand side;

responsive to said first connection name selected from said matching binding entry, identifying a binding table derived security association; and

selectively responsive to said filter derived security association or said binding table derived security association, processing said outbound packet into a tunnel for communication to said remote node.

28. [Original] The program storage device of claim 27, said method steps further comprising:

responsive to said first connection name selected from said matching binding entry and said second connection name comparing not equal, selecting said binding table derived security association for processing said outbound packet.